International Journal of Computing, Communication and Information System(IJCCIS)
Vol 3. No 1. Jan-June 2012 ISSN: 0976 – 1349 pp.18- 20
www.ijcns.com

Study & Analysis of Security Issues inE-commerce Network System

Deepu Saini[1]
Research Scholar, Singhania University, Jhunjhunu, Rajasthan, India
deepu254426@yahoo.com

Dr. Vijay Singh Rathore[2]
PhD (Computer Science), Singhania University, Rajasthan, India
vijaydiamond@gmail.com

***Abstract*-E-commerce systems are based upon internet use, which provides open and easy communications on a global basis. However, because the internet is unregulated, unmanaged and uncontrolled, it poses a wide range of risks and threats to the systems operating on it.The use of the internet means that your internal IT and e-commerce systems are potentially accessible by anyone, irrespective of their location.Privacy – the control over one's personal data – and security – the attempted access to data by unauthorized others – are two critical problems for both e-commerce consumers and sites alike. Without either, consumers will not visit or shop at a site, nor can sites function effectively without considering both.Without trust, most prudent business operators and clients may decide to forgo use of the Internet and revert back to traditional methods of doing business. To counter this trend, the issues of network security at the e-commerce and customer sites must be constantly reviewed and appropriate countermeasures devised.**

These security measures must be implemented so that they do not inhibit or dissuade the intended e-commerce operation. This paper will discuss pertinent network and computer security issues and will present some of the threats to e-commerce and customer privacy. These threats originate from both hackers as well as the e-commerce site itself.

1. INTRODUCTION

While bringing people conveniences, Internet gives rise to the problem of security simultaneously. It's the same that when traditional commercial mode applied on Internet, it brings about many problems of security. The security is of great importance in financial affairs, systems that need high speed verification and authentication, the E-commerce Website and the database etc. As we know, E-commerce is often subjected to the attack and the cheat of hackers. With the development of E-commerce, hacker attacking becomes more and more serious so that it now turns out to be an important aspect that interferes the development of E-commerce. Nowadays Chinese government puts great emphasis on Internet security, and the newly established National Computer & Information Security Management Center is the infrastructure that prompts all levels of work to strengthen the security of network. As the network technology we utilize becomes more advanced so do the security issues surrounding these technologies. Evolving from the days of "sneaker net" to gigabit ethernet has introduced seemingly infinite risks associated with our public and private networks. Access control points, authentication and encryption mechanisms are only a part of the complete solution. As most security administration teams struggles daily to maintain their skill set with the latest breaches, viruses, and vulnerabilities, it is the malicious users that the administrators and consultants are "reactively learning" from. The eradication of trust in Internet commerce applications may cause prudent business operators and clients to forgo use of the Internet for now and revert back to traditional methods of doing business. This loss of trust is being fueled by continued stories of hacker attacks on e-commerce sites and consumer data privacy abuse.

2. THE THREATS TO E-COMMERCE

A. The Threat to Financial Information

People are going to buy products and services from the ecommerce website. In doing so, they are going to share their financial information with an ecommerce website. Such data exchange is constantly under threat. Hackers are constantly on the lookout for an ecommerce website that doesn't have stringent security standards in place. Insecure hosting, more often than not, results in an attempt to access website data without requisite authorization.

B.The Malware Attack

Such attacks are a part and parcel of the life of every website. How often have you heard that a site has been a victim of a virus attack? The result is that the site needs to shut down for maintenance. In the case of an ecommerce website, this leads to tremendous loss of revenue. This is one of those critical security threats that ecommerce website

owners pray that they don't have to face. For this reason, it's important that the ecommerce hosting needs to be malware proof. It's impossible to protect your website against all kinds of virus attacks, but what you could do is make it less susceptible.

C.The threat to Person Identity

An 'identity' is crucial when it comes to buying products and services on an ecommerce website. It includes personal information, interests and preferences and also detailed financial information. Every ecommerce website targets a specific audience and demands a set of information from that audience. At times, the demand is for a comprehensive set of information that creates an online identity for a particular person. If this identity is compromised, the unauthorized user can use the stolen identity for 'n' number of nefarious purposes.

D. Money Thefts

eCommerce services are about transactions, and transactions are very largely driven by money. This attracts hackers, crackers and everyone with the knowledge of exploiting loopholes in a system. Once a kink in the armor is discovered, they feed the system (and users) with numerous bits of dubious information to extract confidential data (phishing). This is particularly dangerous as the data extracted may be that of credit card numbers, security passwords, transaction details etc.Also, Payment gateways are vulnerable to interception by unethical users.

E. Threats to the system

Viruses, worms, Trojans are very deceptive methods of stealing information. Unless a sound virus-protection strategy is used by the eCommerce Solutions firm, these malicious agents can compromise the credibility of all eCommerce web solution services. Often planted by individuals for reasons known best to them alone, viruses breed within the systems and multiply at astonishing speeds. Unchecked, they can potentially cripple the entire system.

F. Authentication

Most notable are the advances in identification and elimination of non-genuine users. Ecommerce service designers now use multi-level identification protocols like security questions, encrypted passwords (Encryption), biometrics and others to confirm the identity of their customers. These steps have found wide favor all around due to their effectiveness in weeding out unwelcome access.

G. Educating Users

eCommerce is run primarily by users. Thus, eCommerce service providers have also turned to educating users about safe practices that make the entire operation trouble free. Recent issues like phishing have been tackled to a good extent by informing genuine users of the perils of publishing their confidential information to unauthorized information seekers.

3. PRIVACY AND SECURITY ISSUES IN E-COMMERCE

Privacy – the control over one's personal data – and security – the attempted access to data by unauthorized others – are two critical problems for both e-commerce consumers and sites alike. Without either, consumers will not visit or shop at a site, nor can sites function effectively without considering both.

A. Privacy

Privacy is a serious issue in electronic commerce, no matter what source one examines. Fisher [2001] reported "Forty-one percent of Web buyers surveyed last year by Forrester Research of Cambridge, Mass., said they have contacted a site to be taken off their databases because they felt that the organization used their information unwisely."
Why this concern about privacy? The answer is simple. As of 1998, the FTC found that the majority of online businesses "had failed to adopt even the most fundamental elements of fair information practices. ([Culnan 2000], p. 8)." Indeed, relatively few consumers believe that they have very much control over how personal information, revealed online, is used or sold by businesses [Culnan and Armstrong 1999]. The combination of current business practices, consumer fears, and media pressure has combined to make privacy a potent problem for electronic commerce.

B. Security

As mentioned, security is also a major concern for e-commerce sites and consumers alike. Consumers fear the loss of their financial data, and e-commerce sites fear the financial losses associated with break-ins and any resulting bad publicity. Not only must e-commerce sites and consumers judge security vulnerabilities and assess potential technical solutions, they must also assess, evaluate, and resolve the risks involved.

4. WHERE IS E-COMMERCE SECURITY HEADING?

Much as there are winners and losers in e-commerce when it comes to the bottom-line results, there will continue to be those who operate a tight ship fending off the sophisticated and random attacks and also those who fall victim from their lack of planning and implementation of defenses. Access to wealth electronically will continue to expand at a frantic pace in electronic transactions over wires and through the air andthe applications that store and process the digital codification of information. It is therefore in the interests of the enablers of these payments to educate their customers to set priorities and methodologies for practicing the best techniques for electronic security.

Recently the Worldwide E-Commerce Fraud Prevention Network was formed by American Express and e-tailers such as Amazon.com and Buy.com to establish common grounds for reducing the threats created by increasing reliance on the Internet for commerce.

5. SECURITY IN E-COMMERCE NETWORK SYSTEM

Some of the recommended strategies for merchants advocated by this group include: obtaining real-time information from a credit card company, use of address verification systems, use of credit card verification codes, purchase of rule-based detection systems, and purchase of predictive statistical models Visa has stepped up a campaign to establish high standards of security for its merchants and cardholders. This was launched in June 2000 as the Global Secure Ecommerce Initiative.

Visa has been actively pursuing the production of smart cards which have a logical chip component to provide enhanced authentication for electronic transactions. Visa uses third-party security assessments to build its own evaluation and weigh these against benchmarks of competitors to develop compliance standards. Visa has also recently launched Global Security Web to serve as an information resource for merchants. This site includes a program for a security self-assessment to help merchants find out what the weak and strong points in preventing unauthorized access to their information.

This is a component that will include seminars and training for merchants to establish compliance in the standards that Visa establishes. By organizing a formal set of rules for compliance, Visa is raising the bar to a level that will benefit all parties in the electronic transaction process.

5. NETWORK INTRUSION DETECTION FOR THE E-COMMERCE ENVIRONMENT

As the demand for E-Commerce grows on the Internet so will the increasing potential for E-Commerce sites to be maliciously attacked. The typically used business impact analysis approach (How much will this cost, if my E-Commerce web server is down) is no longer the standard as a strategic solution for implementing a well-defined security policy for the E-Commerce environment. Organizations also consider different risk factors than that of an insurance security model. The implosion of business on the Internet has created the demand for organizations to take its product and "rush to market". This concept may introduce additional risk(s), a organization that once considered certain risk(s) as unacceptable, may now be acceptable.

With the influx of products being utilized more widely in the E-Commerce environment such as middleware programs, (i.e. Bluestone, MQseries, and Vignette) the need for additional connectivity to critical systems for critical customer data flow is now a requirement in the environment. This data flow may require connectivity to core systems, where a fire walled device may be insufficient. Denial of Service (DoS) and Distributed Denial of Service (DDoS) are becoming increasingly effective tools for malicious users to utilize against E-Commerce Infrastructure, though unknown DoS and DDoS attack may occur, and your organizations Network Based Intrusion Detection may not posture defensively against first time denial of service attacks, IDS can provide you with statistical data for future safeguarding. As we all are aware, but it must be continually emphasized that the majority of security breaches are internal. Monitoring of key segments, internal, and external along with detailed logging and proactive intrusion detection are additional mechanisms in assisting in securing the E-Commerce environment.

REFRENCES

[1]Ackerman, Mark S., and Lorrie Cranor. 1999. Privacy Critics: UI Components to Safeguard Users' Privacy. *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI'99)* : 258-259.

[2] Ackerman, Mark S., Lorrie Cranor, and Joseph Reagle. 1999. Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. *Proceedings of the ACM Conference in Electronic Commerce* : 1-8.

[3] Ackerman, Mark S., Trevor Darrell, and Daniel J. Weitzner. 2002. Privacy in Context. *Human- Computer Interaction*, 16 (2-4) : 167-176.

[4] Andy Briney, "Security Focused,"*Information Security*, September 2000,URL:http://www.infosecuritymag.com/articles/september00/pdfs/Survey1_9.00.pdf